Compression of IPsec AH and ESP Headers for Constrained Environments
draft-raza-6lo-ipsec-02

{shahid.raza, simon.duquennoy}@sics.se
goran.selandaer@ericsson.com
Status of the Document

• First submitted as a position paper to the Smart Object Workshop [RFC6574] co-located with IETF 80.
• Later submitted to 6LoWPAN WG
• Moved to 6lo and included in the 6lo BoF
• Presented in 6lo during the IETF93
Salient Features

- Does not require any modification in the IPsec standard
  - End-to-End compatible with any IPsec enabled hosted on the Internet.
  - Only performs header compression within 6LoWPAN networks without compromising any security properties

- Seamlessly links with the 6LoWPAN standard

- Other compression mechanisms exists
  - draft-mglt-6lo-diet-esp-01 requires changes in the IPsec standard and should also be supported/enabled in hosts on the Internet
  - ROHC [RFC5795][RFC5856]) also targets any Internet hosts and not specific to 6LoWPAN networks
  - Both are complementary to our solution
IP Security (IPsec)

• End-to-end Security at the Network layer
  – Part of the OS
  – Protects IP and UDP/TCP headers
  – IPsec Transport mode for the Internet of Things

• Authentication Header (AH) [RFC-4302]
  – Integrity and authentication

• Encapsulated Security Payload (ESP) [RFC-4303]
  – Confidentiality and optionally integrity and authentication

• AH and ESP are IP extension headers

• IPv6 nodes SHOULD implement IPsec [RFC 6434]
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

BIT 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

0 1 1 TF NH NLIM CID SAC SAM M DAC DAM

IPv6 Header IPv6 Extension Headers UDP UDP Payload
Linking IPsec Headers Compression with 6LoWPAN

IPv6 Header | IPv6 Extension Headers | UDP | UDP Payload
---|---|---|---

Variable Length NHC ID | Compressed next header

Next Header Compression (NHC) [RFC-6282]
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

Next Header Compression (NHC) [RFC-6282]
Linking IPsec Headers Compression with 6LoWPAN

IP Header Compression (IPHC) [RFC-6282]

IPv6 Header
IPv6 Extension Headers
UDP
UDP Payload

Next Header Compression (NHC) [RFC-6282]
Linking IPsec Headers Compression with 6LoWPAN (cont...)

Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header
Linking IPsec Headers Compression with 6LoWPAN (cont...)

Proposal 1 - IPv6 EID:

0: IPv6 Hop-by-Hop Options Header
1: IPv6 Routing Header
2: IPv6 Fragment Header
3: IPv6 Destination Options Header
4: IPv6 Mobility Header
5: Reserved -
6: Reserved -
7: IPv6 Header

**Extension Header Order [RFC2460]**
IPv6 header
Hop-by-Hop Options header
Destination Options header
Routing header
Fragment header
**Authentication header**
Encapsulating Security Payload header
Destination Options header
upper-layer header
Linking IPsec Headers Compression with 6LoWPAN (cont...)

---

**Proposal 1 - IPv6 EID:**

0: IPv6 Hop-by-Hop Options Header  
1: IPv6 Routing Header  
2: IPv6 Fragment Header  
3: IPv6 Destination Options Header  
4: IPv6 Mobility Header  
5: Reserved - IPv6 Authentication Header  
6: Reserved - IPv6 Encapsulated Security Payload  
7: IPv6 Header
Linking IPsec Headers Compression with 6LoWPAN (cont...)

**Proposal 1 - IPv6 EID:**

0: IPv6 Hop-by-Hop Options Header  
1: IPv6 Routing Header  
2: IPv6 Fragment Header  
3: IPv6 Destination Options Header  
4: IPv6 Mobility Header  
5: Reserved - IPv6 Authentication Header  
6: Reserved - IPv6 Encapsulated Security Payload  
7: IPv6 Header

**Proposal 2 - IPv6 EID:**

0: IPv6 Hop-by-Hop Options Header  
1: IPv6 Routing Header  
2: IPv6 Fragment Header  
3: IPv6 Destination Options Header  
4: IPv6 Mobility Header  
5: Reserved  
7: IPv6 Header

*Variable length NHC ID is used to distinguish AH and ESP*
Compressing IPsec (cont...)

- Proposed LOWPAN NHC encoding for AH

```
0 1 2 3 4 5 6 7
+------------------------+
| 1 | 1 | 0 | 1 | SPI | SN |
+------------------------+
```

- Proposed LOWPAN NHC encoding for ESP

```
0 1 2 3 4 5 6 7
+------------------------+
| 1 | 1 | 1 | 0 | SPI | SN |
+------------------------+
```

- SPI: Security Parameter Index
- SN: Sequence Number
## Compressed IPsec AH

<table>
<thead>
<tr>
<th>Octet 0</th>
<th>Octet 1</th>
<th>Octet 2</th>
<th>Octet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Traffic Class</td>
<td>Flow Label</td>
<td></td>
</tr>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
<td>Source Address (128 bits)</td>
</tr>
<tr>
<td>Destination Address (128 bits)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Octet 0</th>
<th>Octet 1</th>
<th>Octet 2</th>
<th>Octet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOWPAN_IPHC</td>
<td>Hop Limit</td>
<td>Source Address (128 bits)</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Compressed IP Datagram secured with compressed AH

IP Datagram secured with AH
## Compressed IPsec AH
(Packet Size comparison)

<table>
<thead>
<tr>
<th>Service</th>
<th>Without IPsec Compression [Byte]</th>
<th>With IPsec Compression [Byte]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity with AH [HMAC-SHA1-96]</td>
<td>12*</td>
<td>4*</td>
</tr>
<tr>
<td>Confidentiality with ESP [AES-CTR]</td>
<td>10**</td>
<td>4**</td>
</tr>
<tr>
<td>Confidentiality and Integrity with ESP [AES-CTR] and [HMAC-SHA1-96]</td>
<td>10***</td>
<td>4***</td>
</tr>
</tbody>
</table>

* Plus 12 bytes of Authentication data
** Plus 8 bytes of Initialization Vector
*** Plus 12 bytes of Authentication data and 8 bytes of Initialization Vector
Compressed IPsec  
(Implementation)

- We implement IPsec in Contiki OS
  - uIPv6 with AH and ESP
  - SICSLoWPAN with AH and ESP
  - Set of standardized cryptographic algorithms
- Even suitable for Class 0 devices [RFC7228]

<table>
<thead>
<tr>
<th>System</th>
<th>ROM (kB)</th>
<th>RAM (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>overall</td>
<td>diff</td>
</tr>
<tr>
<td>Without IPsec</td>
<td>32.9</td>
<td>–</td>
</tr>
<tr>
<td>AH with HMAC-SHA1-96</td>
<td>36.8</td>
<td>3.9</td>
</tr>
<tr>
<td>AH with XCBC-MAC-96</td>
<td>38.4</td>
<td>5.5</td>
</tr>
<tr>
<td>ESP with AES-CBC</td>
<td>41.4</td>
<td>8.5</td>
</tr>
<tr>
<td>ESP with AES-CTR</td>
<td>39.8</td>
<td>6.9</td>
</tr>
<tr>
<td>ESP with AES-XCBC-MAC-96</td>
<td>39.8</td>
<td>6.9</td>
</tr>
<tr>
<td>ESP with AES-CBC + AES-XCBC-MAC-96</td>
<td>41.9</td>
<td>9.0</td>
</tr>
<tr>
<td>ESP with AES-CBC + AES-XCBC-MAC-96</td>
<td>41.9</td>
<td>9.0</td>
</tr>
</tbody>
</table>
IPsec vs. IEEE 802.15.4 security

- Multi hops with 512 byte data size

Questions/Comments

shahid@sics.se

Source Code
svn co https://contikiprojects.svn.sourceforge.net/svnroot/contikiprojects/sics.se/ipsec ipsec